

UNITED STATES PATENT APPLICATION

FOR

PROGRAMMABLE RANDOM BIT SOURCE

Inventor:

Steven E. Wells

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CALIFORNIA 90025
(408) 720-8598

Attorney's Docket No. 042390.P5684

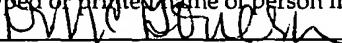
"Express Mail" mailing label number: EM088451912US

Date of Deposit: March 31, 1999

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

Deborah A. McGovern

(Typed or printed name of person mailing paper or fee)


(Signature of person mailing paper or fee)

March 31, 1999

(Date signed)

PROGRAMMABLE RANDOM BIT SOURCE

FIELD OF THE INVENTION

The present invention relates generally to computer security, and more specifically to generating uniform duty cycles in random number generators.

5 BACKGROUND OF THE INVENTION

Random number generator circuits are used in a variety of electronic applications. One important application for random number generators is in the field of computer security where messages are encrypted and decrypted.

10 Cryptography involves the transformation of data into a coded message that is sent to and decoded by only by the intended recipient. Most common cryptographic techniques use ciphers (or "keys") used by the sender to encode the message, and by the receiver to decode the encoded message. Common cipher systems use either a single key to code and decode a message, or two keys, one to encode the message and the other to decode the message.

15 The keys used to encode and decode messages are basically binary data patterns against which a message is processed or filtered. Effective cipher systems require the use of keys that have a sufficiently high number of bits to make replication of a key nearly impossible. Furthermore, the data patterns comprising the keys must be sufficiently random so that their pattern or the
20 patterns in the message encoded by the key cannot be predicted. Effective cryptographic systems thus require the use of high quality random number generators to ensure that the binary data within a message is transformed in a totally unpredictable manner. In general, any lack of randomness in an encryption scheme produces some degree of correlation between the coded and
25 uncoded data. This correlation can then be used to crack the code through techniques such as iterative trial and error predictions of possible output patterns based on a coded message.

A desirable feature of a binary random number generator is that it output one and zero bits in a purely random order. Thus, the value of the output bit at any given time should be totally unpredictable. It is desirable that the duty cycle of the output of the random number generator be approximately fifty percent

5 over an infinite sample size, so that the chance of an output being a logic low (zero) is equal to the chance of the output being a logic high (one). It is also desirable for a random number generator to exhibit low correlation (e.g., approximately zero correlation) between any bit and any other bit, and a flat Fourier distribution among the output bits.

10 Present known random number generators, however, have a tendency to generate an uneven number of zeros or ones over a statistically significant sample size. One cause of unequal duty cycles in certain prior art random number generators is the tendency of latches comprising the random number generator to favor one of the two states. Another cause of unequal duty cycles is

15 a difference between the root-mean square value of the input clock signal and the trip points of the latches.

A common method of decreasing duty cycle variations in random number generators involves the use of a Linear Feedback Shift Register (LFSR) at the output stage of a random bit source. Figure 1 illustrates an example of a prior art random number generator that uses a Linear Feedback Shift Register 104 coupled to the output of a random bit source 102. LFSR 104 comprises a number of latches 105 and gates 106 through which the output bits from random bit source 102 are propagated. The states of the output bits are randomly inverted by gates 106, and the order of the bits is mixed through feed-back of the bits through

20 latches 105.

25

In general, Linear Feedback Shift Registers, such as that illustrated in Figure 1, possess certain disadvantages and do not fully correct non-uniform (or

non-level) duty cycle characteristics exhibited by typical random bit sources. As illustrated by LFSR 104, a typical LFSR itself comprises a number of latches and gates. These latches and gates will tend to exhibit the same propensity to latch a zero or one in certain circumstances, as the latches in the random bit source 102.

5 Therefore, a typical LFSR does not itself produce a uniform duty cycle output of ones and zeros, and thus cannot entirely correct any duty cycle variations in a random bit source.

A further disadvantage of Linear Feedback Shift Registers is the requirement of a large number of latches and gates. For example, a 32-bit LFSR, 10 such as shown in Figure 1, requires 32 D-type latches, as well as a number of combinatorial gates. This adds significantly to the amount of silicon area required for a random number generator circuit that uses such an LFSR.

SUMMARY OF THE INVENTION

One embodiment of the present invention concerns a method of producing a uniform duty cycle output from a random bit source. The method includes testing the duty cycle of said random bit source; varying the output voltage of a voltage source if the duty cycle is not substantially fifty percent; and iteratively altering the output voltage of the voltage source until said duty cycle is substantially fifty percent.

5 Other features and advantages of the present invention will be apparent from the accompanying drawings and from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

5 Figure 1 is a conventional random number generator using a Linear Feedback Shift Register;

Figure 2 illustrates one embodiment of random bit generation by latching a high speed oscillating signal with a low frequency clock signal;

10 Figure 3 illustrates that varying the trip points of a latch can affect the duty cycle output from a random bit source;

Figure 4 is a block diagram of one embodiment of a random bit source;

Figures 5A-5C are embodiments of the programmable voltage source of Figure 4;

15 Figure 6 is a block diagram of another embodiment of a random bit source;

Figure 7 is a block diagram of a computer system including a random number generator incorporating a random bit source;

Figure 8 is a circuit diagram of one embodiment of the programmable voltage source of Figure 4;

20 Figure 9 is a circuit diagram of another embodiment of the programmable voltage source of Figure 4; and

Figure 10 is a circuit diagram of one embodiment of a latch having a bias circuit.

DETAILED DESCRIPTION

A programmable random bit source is described. In one embodiment, a programmable random bit source includes a programmable voltage source, and a latch that samples a high frequency signal with a low frequency clock signal.

5 The duty cycle of the random bit source is determined and, if not substantially fifty percent, the output voltage of the programmable voltage source is varied to adjust the trip point of the latch such that the duty cycle of the random bit source is closer to fifty percent.

It is an intended advantage of embodiments of the invention to provide a
10 circuit that produces a uniform duty cycle for the output of a random bit source. It is a further intended advantage of embodiments of the invention to provide a random number generator that requires a reduced amount of silicon area when implemented in an integrated circuit device.

One method of generating a random pattern of binary digits is to
15 periodically latch a high speed oscillating signal with a lower speed clock signal. Depending on the state of the high frequency signal when the low frequency clock latches, a logic high (one) or a logic low (zero) bit will be produced. Figure 2 illustrates the generation of random bits using a high-speed oscillating signal and a low speed clock. For a general random bit source, the signals represented
20 by waveforms 200 of Figure 2 are input to a D type latch to produce a synchronized output of digital bits.

In Figure 2, waveform 204 represents a high frequency input signal generated by a high speed oscillator. This signal is input to the D input of a D latch. Waveform 202 represents a low frequency clock signal that is input to the
25 clock input of the D latch such that the D latch periodically latches high speed signal 204 at various points. The latched voltage levels of signal 204 are then output from the Q output of the D latch. The high frequency and low frequency

signals are decoupled so that there is no direct relationship between their respective periods.

As illustrated in Figure 2, the low frequency clock signal 202 latches the high frequency signal 204 on negative going clock pulses, 210 - 216. The state of 5 the output bits for each of these pulses corresponds to the position of high speed signal 204 relative to a reference voltage level 206. For a latch-based random bit source, the reference voltage level corresponds to the trip point of the latch. If the high frequency signal is latched while the signal is above the trip point, a logic high is output. Likewise, if the high frequency signal is latched while the 10 signal is below the trip point, a logic low is output.

Preferably, the trip point of the latch corresponds to the root mean square (RMS) value 206 of the high frequency signal 204. In this configuration, the probability of the high frequency signal being latched above the trip point is approximately equal to the probability of the high frequency signal being latched 15 below the trip point. This will produce a random bit source in which the bit correlation between successive output bits is approximately zero, that is, the duty cycle of the output bit waveform will be substantially uniform with an even distribution of ones and zeros.

In some random bit source implementations, a random noise signal is 20 input to the clock input of the latch through a voltage-controlled oscillator. The random noise is typically produced by a random noise source, such as thermal or semiconductor noise. This causes the period of the low frequency clock to vary from pulse to pulse, and adds further randomness to the latching of the high speed signal.

25 In general, however, most present latch-based random bit sources exhibit some non-uniformity in duty cycle. Such non-uniformity is typically due to several factors. One of the main causes of a non-uniform duty cycle is the

tendency of the D latch to latch a particular logic level when data is latched during a forbidden hold or setup time. A second cause of a non-uniform duty cycle is a difference between the RMS value of the high frequency input signal and the trip point of the latch. Another cause may be a non-uniform duty cycle 5 within the high speed oscillator.

Figure 3 illustrates that the trip point of a latch can affect the duty cycle of a random bit source. The RMS level for high frequency signal 302 is shown as line 304. If the trip point of the latch used to latch high frequency signal 302 corresponds to line 306, very few logic high bits will be output compared to the 10 number of logic low bits. Likewise, if the trip point of the latch corresponds to line 308, very few logic low bits will be output compared to the number of logic high bits. In one embodiment of the present invention, a programmable voltage source is used to vary the trip point of the latch to correspond to the RMS level of the high frequency signal.

15 Figure 4 illustrates one embodiment of a programmable random bit source that incorporates a programmable or alterable voltage source to vary the trip point of a latch for the latching of a high frequency signal. Programmable random bit source 400 comprises a D latch 408 which outputs a random distribution of bits from Q output 418. A high speed oscillator 410 is coupled to 20 the D input of D latch 408, and produces a high frequency signal 402 (e.g., signal 204 in Figure 2). A low speed oscillator is coupled to the clock input of D latch 408, and produces a low frequency clock signal 404 (e.g., signal 202 in Figure 2). Programmable random bit source 400 also includes a programmable voltage source 414 (e.g., a voltage trim circuit) coupled to a bias input to D latch 408. The 25 programmable voltage source is configured to vary the trip point of D latch 408 so that high frequency signal 402 is latched by low frequency signal 404 at a desired voltage level of the high frequency signal 402. For one embodiment, the

programmable voltage source is configured to vary the trip point of D latch 408 so that high frequency signal 402 is latched by low frequency signal 404 at the RMS voltage level of the high frequency signal 402.

In one embodiment, latch 408 has a variable trip point. The trip point may 5 be adjusted through a bias circuit included within the latch and controlled by a programmable voltage level output by programmable voltage source 414. Alternatively, a separate bias circuit may be provided that controls the trip point of latch 408 through an input voltage level or similar control signal. The function 10 of such a bias circuit is to adjust the voltage level of the low trip point of latch 408 to a desirable level.

Figure 10 shows latch 1000 that is one embodiment of latch 408 including a bias circuit. Latch 1000 includes bias circuit 1014, CMOS transmission gate 1008, and cross-coupled inverters 1010 and 1012. Bias circuit 1014 includes PMOS transistor 1004 and NMOS transistor 1006 coupled in an inverter 15 arrangement with their gate terminals receiving input data for the latch, and their drain terminals coupled to transmission gate 1008. Bias circuit 1014 also includes PMOS transistor 1002 coupled in series between PMOS transistor 1004 and a power supply voltage. The gate of PMOS transistor 1002 is coupled to a bias voltage (VBIAS) provided by programmable voltage source 414. The trip 20 point of transistor pair 1004 and 1006 may be altered by adjusting VBIAS such that the amount of current supplied to transistor pair 1004 and 1006 is controlled. The voltage output by transistor pair 1004 and 1006 is clocked through transmission gate 1008 by CLK (and its complement CLK#) and latched into cross-coupled inverters 1010 and 1012. Other embodiments of a D latch may be 25 used.

Many different types of programmable or alterable voltage sources may be used for programmable voltage source 414. Figure 8 shows programmable

trim circuit 800 that is one embodiment of programmable voltage source 414.

Programmable trim circuit 800 is an analog circuit that includes differential amplifier 802 and resistors 804 and 806. The non-inverting input of amplifier 802 is connected to ground through pull-down resistor 804, and the inverting input

5 of amplifier 802 is connected to ground through pull-down resistor 806. An analog tuning technique can be implemented by varying the amount of current through the pull down resistors 804 and 806. When the current through pull down resistor 804 is varied, the voltage level input to the non-inverting terminal of amplifier 802 is varied. Similarly, when the current through pull-down resistor 806 is varied, the voltage level input to the inverting terminal of amplifier 802 is varied. In this manner, the output voltage from amplifier 802 can be adjusted. This variable output voltage is then input into a bias input of D latch 408. By adjusting the variable output voltage in amplifier 802, the trip point of D latch 408 can be increased or decreased accordingly.

10 15 The current through the resistors can be varied by varying the resistance of each resistor. This may be accomplished, for example, through use of a laser trimming techniques (e.g., fuses), mask options, or using other programmable circuit elements (e.g., programmable memory elements) to selectively remove or add resistors in parallel or series with resistors 804 and 806.

20 25 Figure 9 shows circuit 900 that is an alternative embodiment of programmable voltage source 414. Circuit 900 is an analog circuit that includes flash memory pair 908 and 910. Flash memory devices utilize a single transistor cell to store one or more bits of data as a function of the amount of charge stored on their floating gates. One important characteristic of flash memory cell is that it is a nonvolatile memory device that retains data even in the absence of a supply voltage. Another important characteristic of a flash memory cell is that

the threshold voltage of the transistor can be easily programmed, read, and/or erased.

Flash memory cells 908 and 910 have their control gates coupled to receive a programming voltage VP on signal line 912. The drain of flash memory cell 5 908 is coupled to a power supply voltage by resistor 904 (or any other current source circuitry), and is also coupled to the non-inverting input of differential amplifier 902. Similarly, the drain of flash memory cell 910 is coupled to the power supply voltage by resistor 906 (or any other current source circuitry), and is also coupled to the inverting input of differential amplifier 902. Amplifier 902 10 senses the difference in the voltage levels at the drains of the flash memory cells and provides an indication of this difference as a voltage level to signal line 416. The drain voltages induced on flash memory cells 908 and 910 are a function of the programmed threshold voltages of the cells. The threshold voltage of each flash memory cell can be individually programmed and/or erased to achieve a 15 desired increase or decrease in the drain voltages. Thus, the drain voltages and the output voltage at signal line 416 can be tuned or programmed to any desirable voltage level.

For certain manufacturing processes, the reference voltage measuring the RMS value of the high frequency input signal may be on the order of 1.0 V to 3.3 20 V. For this reference voltage range, the output voltage of amplifier 902 may be varied on the order of ± 10 mV, depending on the type of devices used, among other factors. The use of flash memory devices allows the bias voltage to be adjusted up or down, and also allows the bias voltage to be set in a non-volatile manner.

25 A digital tuning technique can also be used to implement programmable voltage source 414. For example, one or more CMOS inverters may be used as

shown in Figures 5A-5C. For other embodiments, other logic gates may also be used.

Circuit 500 of Figure 5A includes a CMOS inverter 501 having PMOS transistor 502 and NMOS transistor 504. If both transistors are fabricated with identical current gain characteristics (also referred to as the beta of the transistor), then the output voltage of circuit 501 is approximately $V_{CC}/2$. The transistors may also be fabricated having different current gain characteristics to produce any desirable trimmed voltage. By selectively adding additional pull-up and pull-down transistors, the output voltage can be varied as a proportion of V_{CC} . For example circuit 500 may be expanded through the addition of a number of additional PMOS pull-up transistors, such as transistors 506 and 510 of Figure 5C. Circuit 500 may also be expanded through the addition of a number of additional NMOS pull-down transistors, such as 508 and 512 of Figure 5B. The number and type of transistors added can determine the output voltage of circuit 15 500.

For example, if additional NMOS transistors 508 and 512 are added to input pair 501, as shown in Figure 5B, the output voltage can be varied to any voltage level. If transistors 508 and 512 have the same current gain characteristics as those of transistors 502 and 504, the trimmed output voltage is 20 equal to approximately $V_{CC}/4$. For other embodiments, the current gain characteristics of transistors 508 and 512 may be any other values such that any amount of V_{CC} may be output by the circuit of Figure 5B. Transistors 508 and 512 may be selectively added or removed from the circuit through programmable circuit elements such as fuses (e.g., laser, metal, electrical), masks, or 25 programmable memory elements.

In another example, if additional PMOS transistors 506 and 510 are added to input pair 501, as shown in Figure 5C, the output voltage can be varied to any

voltage level. If transistors 506 and 510 have the same current gain characteristics as those of transistors 502 and 504, the trimmed output voltage is equal to approximately $3V_{CC}/4$. For other embodiments, the current gain characteristics of transistors 505 and 510 may be any other values such that any amount of V_{CC} 5 may be output by the circuit of Figure 5C. Transistors 506 and 510 may be selectively added or removed from the circuit through programmable circuit elements such as fuses (e.g., laser, metal, electrical), masks, or programmable memory elements.

The operation of programmable random bit source 400 of Figure 4 is as follows. The duty cycle of latch 408 is first determined with the output of programmable voltage source 414 set to a neutral or default level (e.g., after reset or power-up). In this case, latch 408 is effectively untrimmed. The output of the programmable voltage source 414 may be monitored by an external tester (e.g., automatic test equipment or "ATE"), other external monitoring circuitry, or by 10 circuitry included in a device with random bit source 400. If the duty cycle is other than approximately 50 percent, the output voltage of programmable voltage source 414 is adjusted. For example, the monitoring circuitry may send one or more control signals to the programmable voltage source or to another circuit to adjust the output voltage from the programmable voltage source (e.g., 15 add or subtract resistors as in Figure 8, program or erase flash memory cells as in Figure 9, or add or remove transistors as in Figures 5B and 5C). This causes the trip point of latch 408 to change accordingly. At this point, the duty cycle of latch 408 is again tested. If the duty cycle is still non-uniform, the output voltage of programmable voltage source 414 is further adjusted. This trial-and-error 20 iterative process of testing the duty cycle, varying the trip point, re-testing the duty cycle is continued until the duty cycle of the latch is approximately 50 percent, or as close as desired to 50 percent. Through this method, the duty cycle 25

of the latch is effectively "tuned" by varying the bias input of the D latch to change the point at which the high frequency signal 402 is latched.

In an alternative method, the duty cycle of latch 408 may be corrected automatically instead of through the iterative method described above. For this embodiment, the non-uniformity of the duty cycle of the untrimmed latch is measured. The variation in duty cycle yields a factor which can be used to determine the adjustment required in the trip point of the latch. This adjustment level is then be translated into a voltage level which is used to determine the adjustment required in the output voltage of programmable voltage source 414.

10 The analog or digital tuning methods described above are then used to adjust the output voltage of programmable voltage source 414 accordingly.

Advantageously, programmable random bit source 400 can be implemented in a much smaller silicon space then a typical Linear Feedback Shift Register circuit (such as that illustrated in Figure 1) because there is no need for a 15 latch per bit output by the random bit source.

Figure 6 illustrates another embodiment of a programmable random bit source 600. Source 600 is a non-deterministic programmable random bit source that includes latch 408 and programmable voltage source 414 as in Figure 4, but has replaced the high speed oscillator with a noise source 602 coupled to 20 comparator circuit 610 through a resistor 604, inductor 606, and capacitor 608. Noise source 602 may be a random noise source, such as thermal or semiconductor noise. The output of comparator 610 is input to latch 408 which is activated by strobe signal 614 to produce digital output 418. The strobe signal may be a clock signal or other signal transition including the low frequency 25 oscillator of Figure 4.

The programmable random bit source previously described above is used in conjunction with a random number generator used to code and decode

messages sent over a computer network. Figure 7 is a block diagram of a computer network for transmitting such encrypted messages. Network 700 includes a sending host computer 702 coupled to a receiving host computer 704 over a network. Both the sending host computer and the receiving host

5 computer contain network interface devices that provide the physical and logical connections between host computer systems and the network medium. Both host computers also contain encryptor/decryptor circuits that perform various cryptographic functions for secure data communication. Sending host 702 includes encryptor/decryptor circuit 706, and receiving host 704 includes

10 encryptor/decryptor circuit 707. The encryptor/decryptor circuits 706 and 707 both include random number generators 708 and 708 that each employ programmable random bit sources 710 ad 711, respectively, such as those of Figures 4 and 6. The random number generators are used to generate the public/private key pairs in public/private key systems.

15 Various methods of data encryption may be used in network 700 to ensure secure communications between sending host 702 and receiving host 704. In one embodiment of the present invention, network 700 uses a public key (asymmetric) cryptographic system. In a public key system, two different keys are used. One key is used by the sender to encode a message and the other key is

20 used by the receiver to decode the coded message. In this system, the encryption (public) key may be widely published, but the decryption (private) key must be kept secret so that only the intended receiver can decode the message. The public and private keys are typically derived together from very large primes and random numbers. Thus, effective random number generators are required

25 to produce truly random key pairs.

In an example of a data transfer using a public key system, sending host 702 composes a message M for transmission to receiving host 704. The two keys

used for the transmission comprise the receiver's public key (PuK_R), and the receiver's private key (PrK_R). The receiver typically selects a public key from a publicly available register of keys, and derives the private key from the public key through a transformation process known only to the receiver. Thus, the 5 correlation between the public key and private key is generally secret and secure. Using the public key, the sending host 702 encodes the message through encryptor/decryptor circuit 706 to create an encoded message M' . Once encoded, only the appropriate private key can decode the message. Upon receiving the message, receiving host 704 decodes the message M' with the 10 private key to recover the original message M .

In one embodiment of the present invention, encryptor/decryptor circuit 707 in receiving host 704 includes random number generator 709 that employs programmable random bit source 711. This technique ensures that the bit distribution from random number generator 709 is sufficiently level and random 15 so that there is no consistent correlation between private and public keys produced by receiving host 704. As shown in network 700, encryptor/decryptor circuit 706 in sending host 702 also includes a random number generator 708 and programmable random bit source 710. This allows sending host 702 to generate secure private keys and public keys when it employs public key transmission. A 20 high degree of randomness is required in generating the key pair so as to make a non-exhaustive search of private keys exceedingly difficult.

In an alternative embodiment of the present invention, network 700 uses a single key (symmetric) system to perform cryptographic functions. In a single-key system, one key is used by both the sender to encrypt the message and by 25 the receiver to decrypt the coded message. This system relies on the secrecy of the key. Therefore, a secure process is required for disclosure of the key only between the sender and receiver and no other party. For this embodiment,

different keys are typically used for different message transactions. Thus, generation of the various keys requires a random process to ensure that a key used for one message transaction cannot be determined from any key used for any other message transaction. For this system the random number generators 5 within the encryptor/decryptor circuits in each of the host computers of network 700 are used to generate the random key patterns for encoding and decoding the message data transmitted between the host computers.

It should be noted that, although embodiments of the present invention have been discussed in relation to single key and public/private key encryption 10 systems, embodiments of the present invention may be used for random number generation in other types of cryptographic systems for secure computer networking. Moreover, the encryptor/decryptor circuits illustrated in Figure 7 may be used in a secure data transmission systems to perform various 15 cryptographic functions such as coding and decoding of messages, authentication of transmitted messages, verification of digital signatures, and other such functions.

In the foregoing, a circuit has been described for producing a uniform duty cycle random number generator. Although the present invention has been described with reference to specific exemplary embodiments, it will be evident 20 that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the invention as set forth in the claims. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.